IN THE CLAIMS

Please amend claims 1-4 and add new claims 5-9 as follows:

1. (CURRENTLY AMENDED) A decryption device[[,]] comprising:

an internal-key storage section operable to store ~~for storing~~ an internal-key;

a content-key storage section operable to store ~~for storing a content-key~~ content-keys;

a determination section operable to determine ~~for determining~~ whether or not a value of the content-key storage section in its initial state and a current value of the content-key storage section are different; and

an operation section, the operation section including:

a first decrypting section operable to [[which]], when an encrypted content-key is input to the operation section, decrypt ~~decrypts~~ the encrypted content-key using the internal-key so as to obtain a content-key and store ~~stores~~ the content-key in the content-key storage section[[,]] and

a second decrypting section operable to [[which]], when an encrypted content is input to the operation section and the determination section determines that the value of the content-key storage section in its initial state and the current value of the content-key storage section are different, decrypt ~~decrypts~~ the encrypted content using the current value of the content-key storage section as the ~~a~~ content-key so as to obtain a first output data and output ~~outputs~~ the first output data to outside of the decryption device.

2. (CURRENTLY AMENDED) A decryption device according to claim 1, further comprising a content-key generation section operable to generate ~~which generates~~ a content-key used for encrypting a content based on random numbers and store ~~stores~~ the generated content-key in the content-key storage section, wherein the operation section further includes:

a first encrypting section operable to encrypt ~~which encrypts~~ the content-key used for encrypting a content so as to obtain an encrypted content-key and output ~~outputs~~ the encrypted content-key to outside of the decryption device[[,]] and

a second encrypting section operable to [[which]], when a content is input to the operation section and the determination section determines that the value of the content-key storage section in its initial state and the current value of the content-key storage section are

different, encrypt ~~encrypts~~ the content using the current value of the content-key storage section as a content-key so as to obtain a second output data and output ~~outputs~~ the second output data to outside of the decryption device.

3. (CURRENTLY AMENDED) A decryption device according to claim 1, further comprising a mutual authentication section operable to determine ~~for determining~~ whether or not a mutual authentication has been made between the mutual authentication section and a storage device which is located outside the decryption device and store ~~stores~~ the encrypted content-key[[,]]

wherein the second decrypting section is operable to decrypt ~~decrypts~~ the encrypted content when the mutual authentication section determines that the mutual authentication has been made.

4. (CURRENTLY AMENDED) A decryption device according to claim 1, wherein:

the internal-key storage section is operable to store ~~stores~~ a plurality of internal-keys; and

the internal-key storage section is operable to select ~~selects~~ one of the plurality of internal-keys as the internal-key based on internal-key selection information input from outside the decryption device to the decryption device.

5. (NEW) A decryption device according to claim 1, wherein:

the second decrypting section is further operable to prevent decryption of the encrypted content when the determination section determines that the value of the content-key storage section in its initial state and the current value of the content-key storage section are the same.

6. (NEW) A method for decrypting encrypted content in a decryption device including an internal-key storage section and a content-key storage section, the method comprising:

storing an internal-key in the internal-key storage section;

storing content-keys in the content-key storage section;

determining whether or not a value of the content-key storage section in its initial state and a current value of the content-key storage section are different; and

decrypting an encrypted content-key provided to the decryption device by using the internal-key so as to obtain a content-key and storing the content-key in the content-key storage section; and

when it is determined that the value of the content-key storage section in its initial state and the current value of the content-key storage section are different, decrypting the encrypted content using the current value of the content-key storage section as the content-key so as to obtain a first output data and outputting the first output data to outside of the decryption device.

7. (NEW) A method according to claim 6, further comprising:

generating a content-key used for encrypting a content based on random numbers and storing the generated content-key in the content-key storage section;

encrypting the content-key used for encrypting the content so as to obtain an encrypted content-key and outputting the encrypted content-key to outside of the decryption device; and

when it is determined that the value of the content-key storage section in its initial state and the current value of the content-key storage section are different, encrypting the content using the current value of the content-key storage section as a content-key so as to obtain a second output data and output the second output data to outside of the decryption device.

8. (NEW) A method according to claim 6, further comprising:

storing a plurality of internal-keys in the internal-key storage section; and

selecting one of the plurality of internal-keys as the internal-key based on internal-key selection information input from outside the decryption device to the decryption device.

9. (NEW) A method according to claim 6, further comprising:

preventing decryption of the encrypted content when it is determined that the value of the content-key storage section in its initial state and the current value of the content-key storage section are the same.